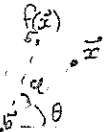
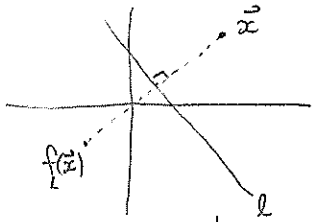
## Rigid Motions of $\mathbb{R}^2$

$f: \mathbb{R}^2 \to \mathbb{R}^2$ which preserves lengths
ie $\forall \vec{x}, \vec{y} \in \mathbb{R}^2$, $\|f(\vec{x}) - f(\vec{y})\| = \|\vec{x} - \vec{y}\|$
these all preserve angles (it can be shown)

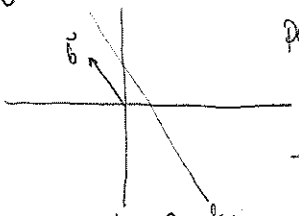
ex ① translations: fix $\vec{b} \in \mathbb{R}^2$, $f_{\vec{b}}: \mathbb{R}^2 \to \mathbb{R}^2$, $\vec{x} \mapsto \vec{x} + \vec{b}$




② rotations: fix $\vec{b} \in \mathbb{R}^2$, fix $\varphi \in [0, 2\pi)$,




③ reflections: reflection through line $\ell$
Any composition of these also
④ glide reflections: fix line $\ell$, fix $\vec{b} \in \mathbb{R}^2$ parallel to $\ell$:



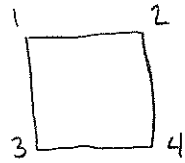

first reflect along $\ell$ then translate by $\vec{b}$

**Theorem:** Every rigid motion of $\mathbb{R}^2$ is either a translation, rotation, reflection, or glide reflection.

As well: A function $f: \mathbb{R}^2 \to \mathbb{R}^2$ is a rigid motion iff $\exists \vec{b} \in \mathbb{R}^2$ and an orthogonal matrix $A \in \mathbb{R}^{2\times 2}$ st $f(\vec{x}) = A\vec{x} + \vec{b}$ $\forall \vec{x} \in \mathbb{R}^2$ (ie $A^T A = I$)

**Def'** Let $G_2$ be the set of all rigid motions of $\mathbb{R}^2$.
Some properties:
① if $f, g \in G_2$ then $f \circ g \in G_2$ (ie $G_2$ is closed under composition)
② if $f \in G_2$ then, $f^{-1} \in G_2$ (ie $G_2$ is closed under taking inverses)
③ $\exists\, id \in G_2$ st $id(\vec{x}) = \vec{x}$ $\forall \vec{x} \in \mathbb{R}^2$ (ie $G_2$ includes identity)

More generally: Let $G_n$ be the set of rigid motions of $\mathbb{R}^n$.
Note $G_n$ satisfies ①-③ as above

ex 


$D_8$ is the set of those permutations of $\{1,2,3,4\}$ which can be obtained by a rigid motion of $\mathbb{R}^2$ which fixes the square
$D_8$ is the dihedral group of order 8 ($\#D_8 = 8$)
Properties: ①-③ as above

More generally, for $n \geq 3$, $D_{2n}$ is the set of perms of $\{1, \dots, n\}$'s obtained by applying rigid motions to a regular $n$-gon. Has properties ①-③. $\#D_{2n} = 2n$

**Def** A group is an ordered pair $(G, \star)$ where

- $G$ is a non-empty set
- $\star : G \times G \to G$ is a binary operation on $G$
- $\star$ is associative: $a \star (b \star c) = (a \star b) \star c \quad \forall a, b, c \in G$
- $\exists e \in G$ st $a \star e = e \star a = a \quad \forall a \in G$
- $\forall a \in G \ \exists b \in G$ st $a \star b = b \star a = e$

2013 01 09

ex ~~$(G_2, \circ)/_{\sim}$~~ $(G_n, \circ)$ $n \geq 2$ } from last day } non-abelian
$(D_{2n}, \circ)$ $n \geq 3$

ex $(\mathbb{Z}, +)$
$(V, +)$ for "vector space" $V$ with its addition } abelian
$(\mathbb{Z}_n, +\bmod n)$

Def) A group $(G, \star)$ is abelian if $a \star b = b \star a$ $\forall a, b \in G$ (ie is commutative).

Def) A group $(G, \star)$ is finite if $G$ is finite, and is infinite otherwise.

Remark: Finite groups are nice because we can write down a table for $\star$

ex $(\mathbb{Z}_4, +)$

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

ex $(\mathbb{Z}_4, \star)$

| $\star$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 3 | 0 | 1 | 2 |
| 2 | 2 | 3 | 1 | 2 |
| 3 | 1 | 2 | 3 | 0 |

To see this is a group,
map $a \mapsto 2a+1$
Now $\star : \{1,3,5,7\} \to \{1,3,5,7\}$
is $\cdot \bmod 8$ so $\star$ is associative.

ex 


$D_8$ exploration:
- let $r$ be the clockwise rotation by 90°
- note $r^2$ is rotation by 180°
- note $r^3$ is clockwise rotation by 270°
- note $r^4$ is the identity
- let $s$ be the reflection through $y=x$
- note $sr$ is reflection through y-axis
- note $sr^2$ is reflection through $y=-x$
- note $sr^3$ is reflection through x-axis

Thus $D_8 = \{1, r, r^2, r^3, s, sr, sr^2, sr^3\}$

| | 1 | r | $r^2$ | $r^3$ | s | sr | $sr^2$ | $sr^3$ |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | r | $r^2$ | $r^3$ | s | sr | $sr^2$ | $sr^3$ |
| r | r | $r^2$ | $r^3$ | 1 | $sr^3$ | s | sr | $sr^2$ |
| $r^2$ | $r^2$ | $r^3$ | 1 | r | $sr^2$ | $sr^3$ | s | sr |
| $r^3$ | $r^3$ | 1 | r | $r^2$ | sr | $sr^2$ | $sr^3$ | s |
| s | s | sr | $sr^2$ | $sr^3$ | 1 | r | $r^2$ | $r^3$ |
| sr | sr | $sr^2$ | $sr^3$ | s | $r^3$ | 1 | r | $r^2$ |
| $sr^2$ | $sr^2$ | $sr^3$ | s | sr | $r^2$ | $r^3$ | 1 | r |
| $sr^3$ | $sr^3$ | s | sr | $sr^2$ | r | $r^2$ | $r^3$ | 1 |

$r^4 = 1$, $s^2 = 1$, $rs = sr^3$

Proposition: Let $(G,\cdot)$ be a group, let $a,b,u,v \in G$.
(i) If $au=av$ then $u=v$.
(ii) If $ua=va$ then $u=v$.
(iii) The equation $ax=b$ has a unique solution.
(iv) The equation $xa=b$ has a unique solution.
Proof: Assume $au=av$. Then $a^{-1}(au)=a^{-1}(av)$, so $(a^{-1}a)u=(a^{-1}a)v$ which yields $eu=ev$. Hence $u=v$. The next is similar.
Assume $x$ is st $ax=b$. Then $a^{-1}(ax)=a^{-1}b$ so $ex=a^{-1}b$ so $x=a^{-1}b$. Hence this is the only possible solution. Also note it is a solution. The next is similar. ∎

Proposition: Let $(G,\cdot)$ be a group, $a,b \in G$.
(i) $(a^{-1})^{-1}=a$.
(ii) $(ab)^{-1}=b^{-1}a^{-1}$.
Proof: Note $(a^{-1})(a^{-1})^{-1}=e=a^{-1}a$. By the above, $(a^{-1})^{-1}=a$.
Note $(ab)(b^{-1}a^{-1})=\cdots=a(bb^{-1})a^{-1})=a(ea^{-1})=aa^{-1}=e$. Similarly $(b^{-1}a^{-1})(ab)=e$. ∎

Fact: Let $(G,\cdot)$ be a finite group. Then each element of $G$ occurs exactly once in each row and column.
applies to infinite groups too... (facepalm)
Proof: Let $a \in G$. Suppose $ab=ac$. Then $b=c$. Suppose $d \in G$. Then $a(a^{-1}d)=\cdots=d$. Similarly for RHS. ∎

Def] Let $(G,\cdot)$ be a group, $a \in G$, $n \in \mathbb{Z}$. Then $a^n := \begin{cases} \underbrace{a\cdots a}_{n \text{ times}} & n \geq 1 \\ e & n=0 \\ (a^{-n})^{-1} & n \leq -1 \end{cases}$

Facts: We have $a^n a^m = a^{n+m}$, $(a^m)^n = a^{mn}$, but in general, $(ab)^n \neq a^n b^n$.

Def] Let $(G,\cdot)$ be a group, $a \in G$. The cycle generated by $a$ is $\langle a \rangle := \{a^n ; n \in \mathbb{Z}\} \leq G$.

Fact: For a group $(G,\cdot)$ and $a \in G$, there are two possibilities.
1) $a^i \neq a^j$ $\forall i \neq j \in \mathbb{Z}$. Then $\langle a \rangle$ is infinite and has "infinite order".
2) $\exists i \neq j \in \mathbb{Z}$ $a^i = a^j$. Then $e = a^{i-j}$. Let $n \in \mathbb{Z}^+$ be least st $a^n = e$. Then $|\langle a \rangle| = n$.
so $\langle a \rangle = \{a^0=e, a^1, \ldots, a^{n-1}\}$

2013 01 14

Recall: For a group $(G,\cdot)$, $a\in G$, we let $\langle a\rangle = \{a^n ; n\in\mathbb{Z}\}$.

Def Let $(G,\cdot)$ be a group, $a\in G$. We let the order of $a$ be $o(a)=|\langle a\rangle|$.

Technically we wrote $o(a)=\begin{cases}\infty & \text{if } |\langle a\rangle| \text{ is infinite}\\ n & \text{if } |\langle a\rangle| = n\end{cases}$

ex Consider $(G,\circ)$. We claim there is an element of every order
- for $n\geq 1$, a rotation by $2\pi/n$ around any point has order $n$
- any translation (non-trivial) has infinite order
- "

ex In $(\mathbb{Z},+)$, $o(0)=1$ and $o(n)=\infty$ $\forall n\in\mathbb{Z}\setminus\{0\}$

ex Consider $(\mathbb{Z}_{18},+)$.

| $a$ | 0 | 1 | 2 | 3 | | $n$ |
|---|---|---|---|---|---|---|
| $o(a)$ | 1 | 18 | 9 | 6 | ... | $\frac{18}{\gcd(n,18)}$ |

number of elements of order $k$ is $\varphi(k)$ for $k\mid 18$

Def Let $(G,\circ)$ be a group, $H\subseteq G$. We say $H$ is a subgroup of $G$ if: ($(H,\circ|_H)$?)
1) $H\neq\emptyset$;
2) $a,b\in H \Rightarrow ab\in H$;
3) $a\in H \Rightarrow a^{-1}\in H$. We write $H\leq G$

ex. $G=(\mathbb{Z},+)$. Claim $H=\{2k : k\in\mathbb{Z}\}$ is a subgroup

ex $G=(\mathbb{Z},+)$, $H=\{0,1\}$. $H\not\leq G$ since $1+1\notin H$

ex $G=(G_2,\circ)$, $H=\{f\in G_2 ; f(\vec{0})=\vec{0}\}$, Exercise: $H$ is a subgroup

Fact: If $(G,\circ)$ is a group and $H\leq G$ then $(H,\circ|_H)$ is a group. Exercise.

Proposition: Let $G$ be a group, $H\subseteq G$. Then $H\leq G$ iff $H\neq\emptyset$ and $a,b\in H\Rightarrow ab^{-1}\in H$.

Proposition: Let $G$ be a group, $H\subseteq G$ finite. Then $H\leq G$ iff $H\neq\emptyset$ and $a,b\in H\Rightarrow ab\in H$.
Proof:

ex. $\langle a\rangle \leq G$ by subgroup criterion, we call $\langle a\rangle$ the cyclic subgroup generated by $a$

Remark: Let $a_1, \dots, a_k \in G$. Then $\exists$ smallest $H \leq G$ st $a_1, \dots, a_k \in H$. (intersect them all)
Denote $H = \langle a_1, \dots, a_k\rangle$.

Def A group $G$ is cyclic if $\exists a \in G$ st $\langle a\rangle = G$.

ex Let $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$. Then $(\mathbb{Z}_n^\times, \cdot \bmod n)$ is a group. ex $\mathbb{Z}_7^\times = \langle 3\rangle$.

2013 01 18

Theorem: Let $G$ be a cyclic group. If $H \leq G$ then $H$ is cyclic.
Proof: If $H = \langle e\rangle$ ok. Else $\exists n > 0$ st $a^n \in H$ (as $a^{-n} \in H$). Let $m$ be the smallest one.
Claim $H = \langle a^m\rangle$. Well $a^m \in H \Rightarrow \langle a^m\rangle \subseteq H$. Now let $h \in H$. Then $h = a^b$. Write $b = qm + r$. Then $h = a^b = a^{qm}a^r = (a^m)^q a^r$. Remains to show $r = 0$. If not, then $a^r = (a^m)^{-q} \cdot h \in H \Rightarrow$ $r \geq m$, contradiction. ∎

Def Let $G$ be a group, $H \leq G$, $a \in G$. The left-coset of $H$ given by $a$ is $aH = \{ah : h \in H\} \subseteq G$. The right-coset of $H$ given by $a$ is $Ha = \{ha : h \in H\} \subseteq G$.

Lemma: Let $G$ be a group, $H \leq G$, $a \in G$. Then $|aH| = |H| = |Ha|$.
Proof: Define $L_a : H \to aH$ by $L_a(h) = ah$. Claim $L_a$ is injective. Suppose $L_a(h_1) = L_a(h_2)$. Then $ah_1 = ah_2 \Rightarrow h_1 = h_2$. Clearly surjective, $\therefore |H| = |aH|$.
Sim. $|Ha| = |H|$. ∎

Def Let $G$ be a group, $H \leq G$, $a, b \in G$. Say $a \equiv_L b \pmod H$ if $a^{-1}b \in H$.
Remark: This is an equivalence class. (exercise) $\to$ equivalence classes $[a]_L^H$

Proposition: Let $G$ be a group, $H \leq G$, $a \in G$. Then $aH = [a]_L^H$.
Proof: Let $x \in [a]_L^H$. So $a \equiv_L x \pmod H \Rightarrow a^{-1}x \in H \Rightarrow a^{-1}x = h$ for some $h \in H \Rightarrow x = ah \Rightarrow x \in aH$. $\Rightarrow [a]_L^H \subseteq aH$
Let $x \in aH$. So $x = ah$ some $h \in H$. Then $a^{-1}x = h \Rightarrow a^{-1}x \in H \Rightarrow a \equiv_L x \pmod H$
$\Rightarrow x \in [a]_L^H \Rightarrow aH \subseteq [a]_L^H \Rightarrow aH = [a]_L^H$. ∎

Remark: $\{aH : a \in G\}$ is a partition of $G$, $a \equiv_L b \pmod H$ iff $aH = bH$.

We can also do this on the right.
Def) $a \equiv_R b \pmod H$ if $ba^{-1} \in H$
Again we will find $\equiv_R \pmod H$ is an equivalence relation.
$[a]_R^H = \{x \in G ; a \equiv_R x \pmod H\} = Ha$ (exercise)
The right cosets of H also partition G.
In general, these partitions are different.
Recall, $|aH| = |H| = |Ha|$.

Theorem (Lagrange's Theorem): Let G be a finite group, $H \leq G$. Then $|H| \mid |G|$.
Proof: $|G| = \sum_{i=1}^{k} |aH| = \sum_{i=1}^{k} |H| = k|H|$ where $a_1H, \dots, a_kH$ are the left cosets. ∎

Def) Let G be a group, $H \leq G$. The index of H in G, denoted $[G:H]$, is the number of left cosets of H in G.

Corollary: If G is a finite group, $H \leq G$, then $[G:H] = |G|/|H|$ ∎

Corollary: Let G be a finite group, $a \in G$. Then $|a| \mid |G|$.
Proof: Well $|a| = |\langle a \rangle|$. As $\langle a \rangle \leq G$, we have $|\langle a \rangle| \mid |G| \Rightarrow |a| \mid |G|$. ∎

Corollary: Let G be a group, $|G| = p$, p prime. Then G is cyclic.
Proof: Note $|G| \geq 2$, so pick $a \in G \setminus \{1\}$. Then $a \neq 1$ so $|a| > 1$. But $|a| \mid p$, so $|a| = p$. Hence $|\langle a \rangle| = p \Rightarrow \langle a \rangle = G$. ∎

Corollary: Let G be a finite group, $H_1, \dots, H_k \leq G$. If $\gcd(|H_1|, \dots, |H_k|) = 1$ then $\bigcap_{i=1}^{k} H_i = \{1\}$.
Proof: Suppose $a \in \bigcap_{i=1}^{k} H_i$. Then $a \in H_i$, so $|a| \mid |H_i|$. $\therefore |a| \mid \gcd(|H_1|, \dots, |H_k|)$, so $|a| = 1 \Rightarrow a = 1$. ∎

Def) Let G be a group, $A, B \subseteq G$. Then $AB = \{ab ; a \in A, b \in B\} \subseteq G$.

Proposition: Let G be a group, $H, K \leq G$ finite. Then $|HK| = |H||K| / |H \cap K|$.
Proof: Observe $HK = \bigcup_{h \in H} hK$. Note $h_1K = h_2K$ iff $h_1^{-1}h_2 \in K$ iff $h_1^{-1}h_2 \in K \cap H$ iff $h_1(K \cap H) = h_2(K \cap H)$. So the # of left cosets of K in G named by $h \in H = [H : H \cap K] = |H| / |H \cap K|$. So $|HK| = (|H| / |H \cap K|)|K|$. ∎

ex. $D_6 = \{1, r, r^2, s, sr, sr^2\}$ $|\langle s \rangle| = |\langle sr \rangle| = |\langle sr^2 \rangle| = 2$ $|\langle s \rangle \cap \langle sr^2 \rangle| = 1 \Rightarrow |\langle s \rangle \langle sr^2 \rangle| = 4$ ($4 \nmid 6 \Rightarrow$ not subgroup)

2013 01 23

**Def** Let $\Omega$ be a non-empty set. Define the symmetric group $S_\Omega := \{f : \Omega \to \Omega \text{ a bijection}\}$.

Fact: $(S_\Omega, \circ)$ is a group.

Remark: When $\Omega = \{1, \dots, n\}$, we write $S_n$.

Notes: $S_n$ is the symmetric group of degree $n$, $|S_n| = n!$ Notation for elements:

ex

| $x$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| $\sigma(x)$ | 4 | 8 | 6 | 3 | 5 | 1 | 2 | 7 |

write $(1\,4\,3\,6)(2\,8\,7)(5)$ (cycles)

not unique

Conventions: Don't write 1-cycles